# OSINT-X: Domain Intelligence and Exposure Analysis Dashboard

**A. AMBICA[1],VEMULAMADA DAVYA POOJITHA [2] , VENDRA NAVEENA[3], VOODIKILA AMULYA[4], ANAKAPALLI GUNA [5]**

[1] *Professor , Department of Information Technology and Computer Applications Engineering, Andhra University College of Engineering for Women, Andhra Pradesh, India*

[2345] *Students, Department of Information Technology and Computer Applications , Andhra university college of engineering for women ,Visakhapatnam - 530003, AP India*

***Abstract*—Open Source Intelligence (OSINT-x) plays an important role in cybersecurity by collecting publicly available information from the internet. Many organizations unknowingly expose sensitive information such as domain details, email addresses, DNS records, and open ports, which can be misused by attackers during the reconnaissance phase of cyber attacks.**

***This project focuses on developing an OSINT-x based information gathering system that collects and analyses publicly available data related to a target domain. The system integrates multiple modules to gather information such as DNS records, subdomains, email addresses, IP information, and open services. The collected data is then organized and presented in a structured format to help understand the digital exposure of an organization.***

***This paper presents OSINT-X, an integrated OSINT-based domain intelligence and exposure assessment framework designed to automate reconnaissance and risk evaluation processes. The proposed system consolidates multiple modules, including WHOIS lookup, DNS enumeration, subdomain discovery, email extraction, port scanning, SSL certificate analysis, reverse IP lookup, HTTP header inspection, and network profiling, into a unified architecture. The system collects structured intelligence from publicly available sources and processes it through a centralized Threat Engine that performs correlation analysis, exposure scoring, and risk simulation.***

***The architecture follows a modular and layered design to ensure scalability, maintainability, and efficient data processing. Experimental evaluation demonstrates that OSINT-X successfully identifies potential exposure points and generates actionable security insights through an interactive dashboard and automated PDF reporting mechanism. By integrating automated data collection with risk-based analysis, the proposed framework enhances cybersecurity awareness and assists organizations in proactively identifying vulnerabilities before exploitation.***

***Keywords*— Open Source Intelligence (OSINT), Domain Intelligence, Cybersecurity, DNS Analysis, WHOIS, Subdomain Enumeration, Port Scanning, SSL Certificate Analysis, Threat Detection, Risk Assessment, Digital Exposure, Reconnaissance.***

## 1. Introduction

With the expansion of digital services , online. During reconnaissance, attackers gather publicly available data such as DNS records, WHOIS details, email addresses, and open ports. OSINT-X provides an automated and structured platform to evaluate such exposure ethically. OSINT-X is an open-source web-based intelligence collection tool that has been built on Python and Flask framework. The system enables users to do automated reconnaissance on a certain domain by gathering data of several publicly available sources including WHOIS databases, DNS servers, web pages, certificate transparency logs, and network information services. OSINT-X will combine these functions into one centralized dashboard as opposed to using a series of independent tools.

The main interest of the system is to have a clear and structured picture of the exposure of a domain. The data gathered is in both raw and visual form, which allows its users to interpret the results in an easy way including the exposed email addresses, subdomains, open ports and security misconfigurations. Reports can also be generated in the platform hence it is appropriate in academic documentation and analysis.

With the rapid growth of the internet and digital services, organizations increasingly rely on online platforms for communication, business operations, and data management. However, this digital presence also leads to the exposure of a large amount of publicly available information on the internet. This information can be collected using Open Source Intelligence (OSINT) techniques without directly interacting with the target system.

In cybersecurity, the first phase of many cyber attacks is **reconnaissance**, where attackers gather publicly available information about a target organization. This information may include domain details, DNS records, IP addresses, subdomains, email addresses, and open network services. Such data can help attackers understand the structure of a target system and identify potential vulnerabilities. The main objective of this project is to develop an OSINT-based information gathering system that collects publicly available information related to a domain and presents it in a structured format. By analysing this data, organizations can understand their digital exposure and take necessary steps to improve their cybersecurity posture. This project demonstrates how publicly accessible information can provide valuable insights for both security professionals and organizations.

## 1. Literature Review

Open-Source Intelligence (OSINT) has become an essential technique in modern cybersecurity and digital investigations. According to Exploring OSINT for Modern Day Reconnaissance, OSINT focuses on collecting and analysing information from publicly available sources such as websites, DNS records, social media platforms, and domain registration databases. These sources provide valuable intelligence that can be used for reconnaissance, threat analysis, and security assessments. The study highlights that OSINT plays a critical role in the reconnaissance phase of cybersecurity, where analysts gather information about a target organization before conducting further security evaluation.

Researchers have also emphasized that OSINT tools allow security analysts to gather large volumes of publicly accessible data and convert it into meaningful intelligence through structured processes such as data collection, processing, analysis, and reporting. This intelligence cycle helps organizations detect potential vulnerabilities and improve their security posture.

Recent studies further indicate that integrating automated techniques and machine learning with OSINT systems can significantly improve the efficiency of data analysis. Artificial intelligence can assist in clustering, classification, and identifying patterns in large OSINT datasets, which enhances the ability to detect malicious activities or suspicious domains.

Overall, previous research demonstrates that OSINT-based frameworks are widely used in cybersecurity, digital investigations, and threat intelligence. However, many existing tools lack integrated platforms that combine multiple OSINT modules for automated analysis and reporting. This limitation motivates the development of systems like OSINT-X, which aim to provide a unified platform for collecting, processing, analysing, and presenting publicly available intelligence related to a target domain.

## 3. Methodology

The approach taken in the current project commences with the introduction of a target domain by the user using the web interface. The system collects data based on the modules selected in the format of API, DNS queries and HTTP requests. The collected information is standardized into tabular forms and presented on the dashboard. Visual charts are created to indicate patterns of exposure and a consolidated report could be exported to be documented.

## 4. System Architecture and Design

The general design, architecture, and approach to development of the OSINT-X Domain Intelligence Gathering and Exposure Evaluation System are explained. These are modular and layered architecture that is made to allow the system to be scaled, readable, and maintainable. All the design elements help in the effective gathering, processing and visualization of domain intelligence information.

### 4.1 Architectural Design / System Flow

OSINT-X is client-server based. The user interface with the system is a web-based graphical user interface (GUI), and the backend performs data collection and processing as OSINT-X. The Flask web framework is the main controller where the input of the user is received, the chosen modules are launched, the results are collected, and the output is presented.

The general system process commences with the user visiting a target domain and choosing the modules needed to carry out the scanning. The backend further executes each of these modules separately and gathers information on public sources. The results of the processes are processed and stored in structured format and displayed on the dashboard with visual analytics and report download options.

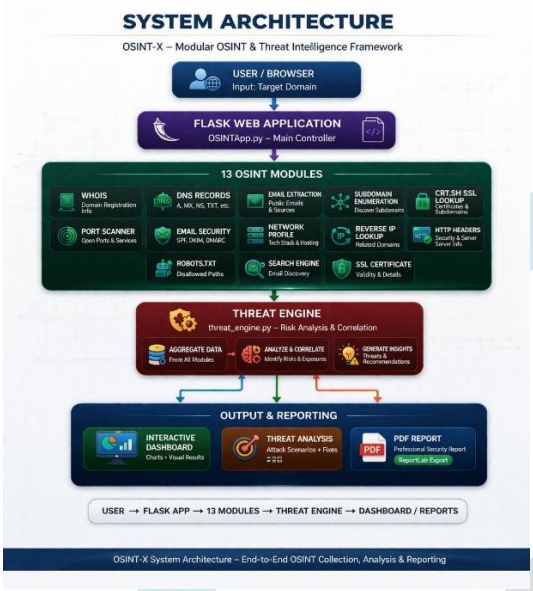



Fig no.4.1 System Architecture

### A. Presentation Layer

The Presentation Layer consists of a web-based user interface through which users provide a target domain for analysis. This layer is responsible for handling user interaction and displaying processed results in a structured dashboard format.

### B. Application Layer

The Application Layer is implemented using the Flask web framework. The main controller (OSINTApp.py) manages routing, request handling, and coordination between OSINT modules and the Threat Engine. It ensures proper workflow execution and structured data transfer between components.

### C. OSINT Processing Layer

The OSINT Processing Layer contains multiple independent modules responsible for intelligence gathering. These include:

- WHOIS Information Retrieval
- DNS Record Enumeration
- Subdomain Discovery
- Email Extraction
- Port Scanning
- SSL Certificate Analysis
- CRT.SH Certificate Transparency Lookup
- Reverse IP Lookup
- HTTP Header Analysis
- Robots.txt Inspection
- Network Profiling
- Email Security Analysis
- Search Engine-based Email Discovery

Each module collects publicly available data and converts it into structured output for further processing.

### D. Threat Intelligence Layer

The Threat Intelligence Layer consists of a centralized Threat Engine (threat_engine.py). This component performs correlation analysis on collected data, evaluates exposure severity, simulates possible attack scenarios, calculates risk scores, and generates remediation recommendations.

### E. Output Layer

The Output Layer presents the analysed information through:

1. Interactive Dashboard (charts and structured results)
2. Threat Analysis Summary (risk level and attack simulation)
3. Automated PDF Security Report

## 5. Implementation

The OSINT-X system is implemented using Python and the Flask web framework, following a modular and layered development approach. The implementation focuses on automated intelligence gathering, structured data processing, and risk-based analysis.

### A. Development Environment

The system is developed and tested in a Linux-based environment (Kali Linux) using Python 3.x. A virtual environment is configured to manage dependencies. Required libraries such as whois, dnspython, socket, requests, ssl, and BeautifulSoup are installed for OSINT data collection and processing.

### B. Frontend Implementation

The user interface is developed using HTML, CSS, and basic JavaScript. The frontend provides:

- Domain input field
- Scan configuration options
- Results dashboard
- PDF report download feature

The interface communicates with the Flask backend through HTTP requests.

**C. Backend Implementation**

The backend is implemented using Flask (OSINTApp.py), which acts as the main controller. It handles:

- User input validation
- Routing requests to OSINT modules
- Collecting module outputs
- Passing structured data to the Threat Engine

Each OSINT module is implemented as a separate Python file inside the modules directory, ensuring modularity and scalability.

**D. OSINT Module Implementation**

Each module performs a specific reconnaissance task:

- WHOIS Module: Retrieves domain registration details.
- DNS Module: Extracts DNS records such as A, MX, NS, and TXT.
- Subdomain Module: Identifies publicly available subdomains.
- Email Module: Extracts exposed email addresses from web content.
- Port Scan Module: Detects open network ports using socket connections.
- SSL Module: Retrieves certificate information and encryption details.
- Reverse IP Module: Identifies domains hosted on the same IP address.
- HTTP Header Module: Analyses server header information.
- Robots.txt Module: Extracts publicly accessible directories.
- Network Profile Module: Collects IP and hosting details.

Each module returns structured JSON-like output for further analysis.

**E. Threat Engine Implementation**

The Threat Engine (threat_engine.py) processes the collected OSINT data and performs correlation analysis. It:

- Evaluates exposure severity
- Calculates exposure score
- Simulates possible attack scenarios
- Generates remediation recommendations

This converts raw reconnaissance data into actionable security intelligence.

**F. Report Generation**

The system generates a structured PDF report using a reporting library. The report includes:

- Domain details
- Module results
- Threat analysis
- Exposure score
- Security recommendations

## 6. Results


Fig.1 Home Dashboard

The system of OSINT-X has a home dashboard as illustrated in the above figure. This screen is the main one that the user will be interacting with the application. The dashboard gives the user the ability to put the targeted domain name, scan profile option, and to turn or off several OSINT modules like the WHOIS, DNS records and email extraction, subdomain scanning, and analysis of the SSL. The dashboard is also made in a clean and intuitive layout to make it easy to use. The flexible selection modules are flexible and enable the user to scan flexibly depending on their needs. An intelligence-gathering process is triggered by a special scan execution button.

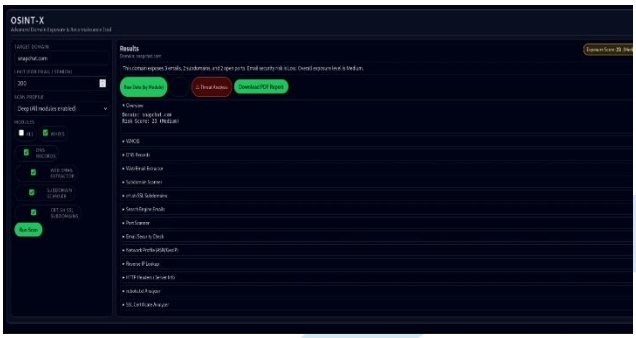


Fig.2.Raw Results

OSINT-X system displays the raw results in the panel. This section represents the raw intelligence data that was obtained immediately after the scan as acquired through different sources in the society. The raw findings comprise of WHOIS information, DNS information, identified subdomains, and retrieved email addresses. The display of raw data enables more sophisticated users to confirm that the information collected is trustworthy and conduct their own analysis of the collected information. This panel will guarantee transparency in the OSINT process as it will display the actual data that has been retrieved prior to any correlation or exposure analysis.

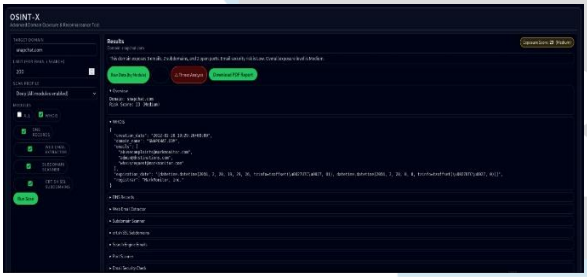


Fig .3. Module-wise Detailed Output

The detailed output of figure above represents the module-wise output of the OSINT-X system. The results of each OSINT module are presented in a dedicated expandable section, which simplifies the process of users analysing certain components of intelligence separately. Services like WHOIS analysis, DNS enumeration, web email mining, subdomain discovery, and port scanning are modules that give detailed results of the selected domain. This organized display enhances the readability and enables the users to gain a clear picture of the contribution of each module to the entire exposure assessment. It also assists in documenting academics, as it enables the results to be interpreted according to the module.

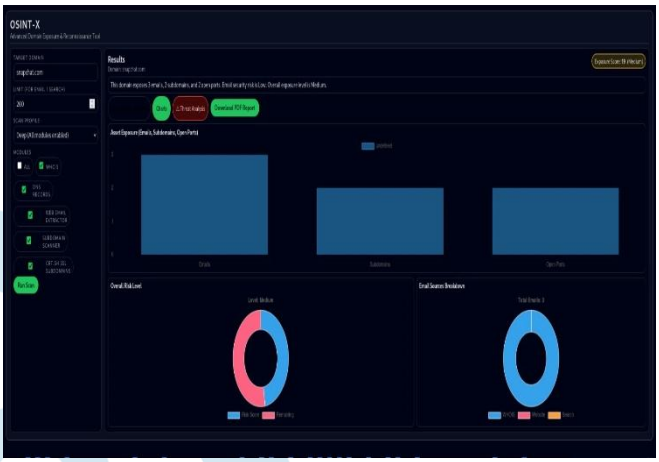


Fig.4. Visual Analytics Dashboard

The visual analytics dashboard of the OSINT-X system is depicted above figure. This screen represents the analysed intelligence information in visual format with the help of charts and visual signs. The dashboard presents the most important metrics related to exposure like the amount of discovered emails, subdomains, open ports, and the total exposure score. Presentation of information in the form of a graph allows the user to understand the level of risk related to the target domain in a quicker manner. The analytics dashboard will improve decision-making because it will convert complex intelligence information into visual insights that are easy to comprehend.

Sample test case execution output of the OSINT-X system showing exposure score, identified attack scenarios, and remediation recommendations.

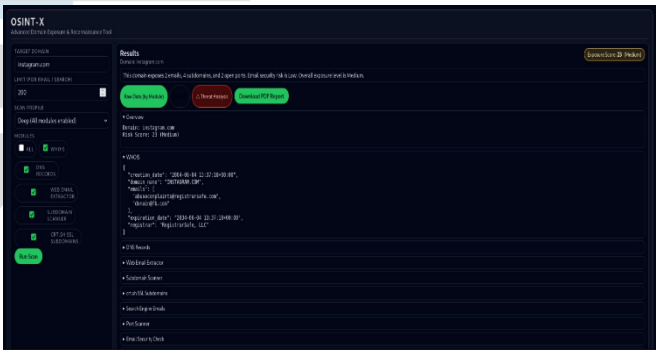
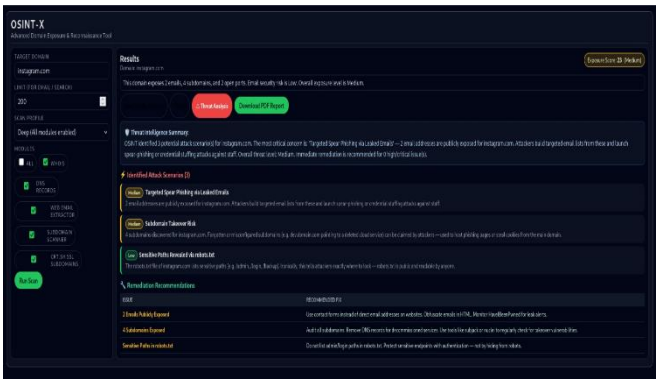


Fig.5. Sample Test Case Execution Output

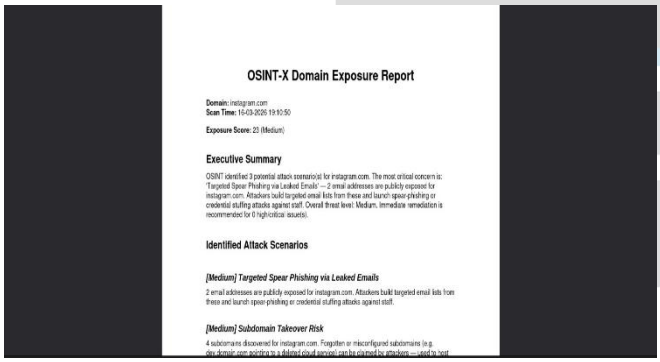


To evaluate the effectiveness of the proposed OSINT X framework, multiple test cases were executed using publicly available domain names. Figure illustrates the

sample execution output generated by the system . Upon providing a target domain as input, the system successfully performed intelligence gathering using all enabled OSINT modules. The results include domain registration details, DNS records, discovered subdomains, exposed email addresses, SSL certificate information, and identified open ports .The Threat Intelligence Summary section highlights the identified exposure points and categorizes them based on severity level (Low, Medium, High). The system further simulates possible attack scenarios such as:Targeted spear phishing via leaked email addresses Subdomain takeover risk Sensitive path exposure through robots.txt An exposure score is calculated based on the identified vulnerabilities. The system also generates remediation recommendations for each issue, providing actionable mitigation strategies.

The execution output demonstrates that OSINT-X effectively consolidates reconnaissance data into a structured dashboard and produces a downloadable PDF security assessment report. The results validate the system's capability to transform publicly available domain intelligence into meaningful cybersecurity insights.

**Automatically generated OSINT-X domain exposure PDF report:**


OSINT-X Domain Exposure Report

Domain: instagram.com
Scan Time: 16-03-2026 19:10:50

Exposure Score: 23 (Medium)

Executive Summary

OSINT identified 3 potential attack scenario(s)d for instagram.com. The most critical concern is: Targeted Spear Phishing via Leaked Emails' — 2 email addresses are publicly exposed for instagram.com. Attackers build targeted email lists from these and launch spear-phishing or credential stuffing attacks against staff. Overall threat level: Medium. Immediate remediation is recommended for 0 high/critical issue(s).

Identified Attack Scenarios

*[Medium] Targeted Spear Phishing via Leaked Emails*

2 email addresses are publicly exposed for instagram.com. Attackers build targeted email lists from these and launch spear-phishing or credential stuffing attacks against staff.

*[Medium] Subdomain Takeover Risk*

4 subdomains discovered for instagram.com. Forgotten or misconfigured subdomains (e.g. dev.domain.com pointing to a deleted cloud server) can be claimed by attackers — used to host

Fig.6. PDF REPORT GENERATION

The OSINT-X system includes an automated PDF report generation module that produces a structured and downloadable security assessment document. This feature enables users to export domain intelligence findings in a professional and shareable format. After the completion of the reconnaissance and threat analysis phases, the processed results are passed to the report generation module. The system dynamically formats the collected data into predefined report sections, including:

Domain Information
Executive Summary
Exposure Score
Identified Attack Scenarios
Risk Classification
Remediation Recommendations

The report generation process ensures that all intelligence gathered from multiple OSINT modules is consolidated into a single comprehensive document. The PDF is structured to resemble a professional cybersecurity audit report, making it suitable for organizational review and documentation purposes.

## 7. Conclusion

The project OSINT-X Domain Intelligence Gathering and Exposure Evaluation System was successfully designed and deployed with the aim of offering a holistic, ethical and educational system of intelligence analysis based on domains to open-source. In the present-day digital environment, where organizations and individuals gain more and more reliance on internet-facing services, the knowledge about the publicly available information of a domain has become a sensitive element of cybersecurity. The project meets that requirement by providing a non-invasive and systematic system to assess the exposure to the domain with the help of OSINT methods. The OSINT-X system is a good illustration of the way in which publicly available information may be obtained, processed, and represented in a significant way without stepping over the legal or moral limits. The system also promotes adherence to the best practices of cybersecurity since it relies solely on open-source intelligence, which enhances the significance of responsibleness. The project points out that there is a lot of knowledge regarding the digital of an organization. footprint is found without active use or pirating activities. The modular design architecture is also one of the major strengths of the OSINT-X system. All functions of intelligence gathering (WHOIS analysis, DNS enumeration, email extraction, subdomain discovery, SSL certificate investigation, port scanning, email security evaluation) are deployed as autonomous modules. This modular model enhances the system maintainability, ease of debugging and enables future improvements that may be added with minimum effect on the current functionality. The architecture is also scalable and enables the system to be dynamic and able to support a changing cybersecurity requirement.

## 8. References

1.Leveraging OSINT for Advanced Proactive Cybersecurity: Strategies and Solutions
https://ieeexplore.ieee.org/document/11143131
2. Open Source Intelligence for Malicious Behavior Discovery and Interpretation
https://ieeexplore.ieee.org/document/9566808
3. Who are you? OSINT-based Profiling of Infrastructure Honeypot Visitors
https://ieeexplore.ieee.org/document/10131856
4. The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends
https://ieeexplore.ieee.org/document/8954668
5. 11 OSINT for Digital Forensics Investigations
https://ieeexplore.ieee.org/document/10643799
6. Exploring OSINT for Modern Day Reconnaissance
https://ieeexplore.ieee.org/document/10420426
7. Use of Open-Source Intelligence in cybersecurity reconnaissance
https://ieeexplore.ieee.org/document/10420426
8. Challenges in OSINT tools and frameworks
https://ieeexplore.ieee.org/document/10212168
9. DCC-Find: DNS Covert Channel Detection by Features Concatenation-Based LSTM: DNS Covert Channel Detection
https://ieeexplore.ieee.org/document/10063732
10. Measuring IPv6 DNS Reconnaissance Attacks and Preventing Them Using DNS Guard**:** DNS Reconnaissance Attacks
https://ieeexplore.ieee.org/document/8416497
11. Understanding Domain Registration Behavior through WHOIS Data Analysis: WHOIS Information Analysis
https://ieeexplore.ieee.org/document/9152777
12. A Measurement Study of Domain Names and DNS Infrastructure: Subdomain Discovery Techniques
https://ieeexplore.ieee.org/document/7347834
13. Detecting Malicious Domains Using DNS Data Analysis
https://ieeexplore.ieee.org/document/7781635
14. Internet-Wide Scanning and Reconnaissance Techniques
https://ieeexplore.ieee.org/document/8464906
15. Open Source Intelligence for Cyber Security Assessment
https://ieeexplore.ieee.org/document/9050163